Agility 2018 Hands-on Lab Guide

Contents:

1 Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

Note: All work for this lab will be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

1.1 Lab Topology

The following components have been included in your lab environment:

- 1 x F5 BIG-IP AFM VE (v13.1.0.6)
- 2 x vyOS routers (v1.1.8)
- 1 x Flowmon Collector (v9.01.04)/DDoS Defender (v4.01.00)
- 1 x Webserver (Ubuntu 16.04)
- 1 x Jumphost (Windows 7)
- 1 x Attacker (Ubuntu 16.04)

1.1.1 Lab Components

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Connection Type, Credentials
Jumphost	• **Management:** 10.1.1.199 • **Users:** 10.1.10.30 • **Internal:** 10.1.20.30 • **Servers:** 10.1.30.30	RDP `external_user`/`P@ssw0rd!`
BIG-IP AFM	• **Management:** 10.1.1.7 • **Internal:** 10.1.20.245	TMUI `admin`/`admin`
Flowmon Collector/DDoS Defender	• **Management:** 10.1.1.9 • **Internal:** 10.1.20.10	TMUI `admin`/`admin`
Router 1	• **Management:** 10.1.1.10 • **Users:** 10.1.10.243 • **Internal:** 10.1.20.243	ssh `vyos`/`vyos`
Router 2	• **Management:** 10.1.1.11 • **Users:** 10.1.10.244 • **Internal:** 10.1.20.244	ssh `vyos`/`vyos`
Attacker	• **Management:** 10.1.1.4 • **Users:** 10.1.10.100	ssh `f5admin`/`f5admin`
Webserver	• **Management:** 10.1.1.6 • **Servers:** 10.1.30.252	ssh `f5admin`/`f5admin`

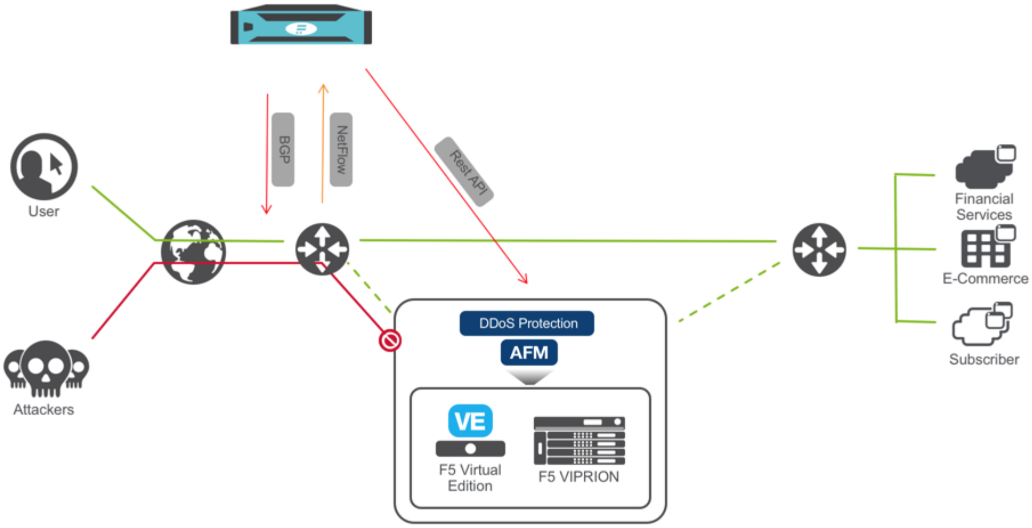
2 Module – Deployment use case and Lab diagram

In this module you will learn about common use-case for AFM/DHD + Flowmon out-of-path DDoS protection solution and explore Lab diagram.

2.1 Deployment use case

A Joint F5 + Flowmon solution is deployed "out-of-path" and provides an out-of-band DDoS mitigation of L3-4 volumetric DDoS attacks. It's a simple and convenient solution that leverages the existing IT infrastructure to provide traffic flow information.

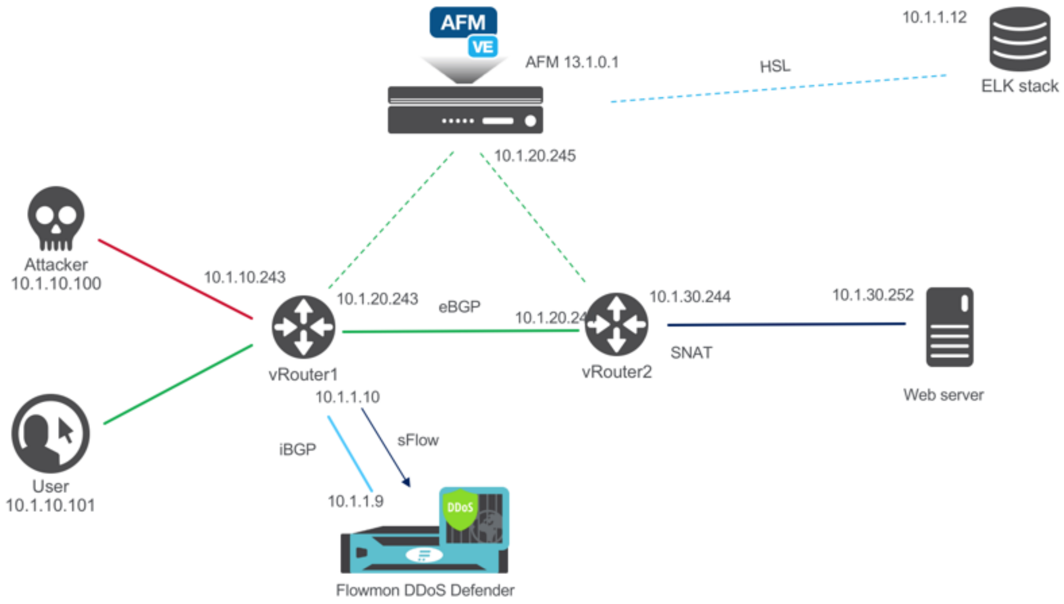
Flowmon Collector appliance receives NetFlow/sFlow/IPFIX from edge routers while Flowmon DDoS Defender uses i/eBGP/Flowspec to route the traffic to F5 DHD/AFM appliance. F5 DHD/AFM DDoS profile, VS and other parameters provisioned dynamically through iControl REST.



Pic.1 Solution Diagram

2.2 Lab blueprint setup

Lab blueprint is deployed in Oracle Ravello cloud with access from F5 UDF portal. All Flowmon elements are pre-configured, F5 AFM VE resources are provisioned and network is configured.



Pic.2 Lab blueprint

2.3 Licensing

BIG-IP is licensed automatically.

Evaluation license has been applied to Flowmon Collector/DDoS Defender. Please contact Lab admin if there are issues with any lab elements.

2.4 Other considerations

Note: Router1 is configured to export sFlow with sampling rate of 1

Note: Learn about sFlow:

https://sflow.org

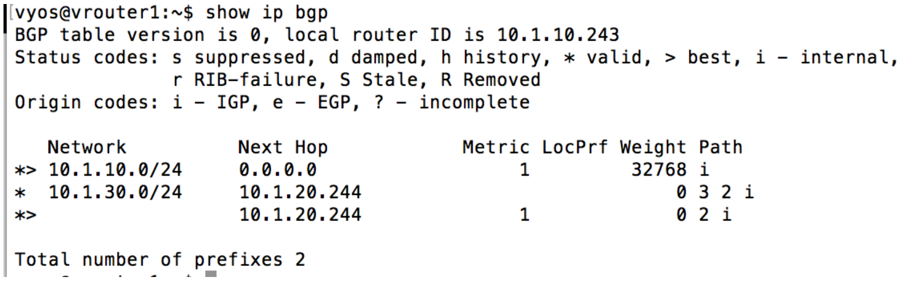
3 Module – DDoS Attack

In this module you will prepare for and launch a SYN flood DoS attack. You will need an active RDP connection to a Linux Jumphost to perform all necessary prerequisites

3.1 Prepare traffic visualization and monitoring

- Connect to Windows jumphost using RDP
- Open SSH connections to Router1 and Router2
- **Verify Router1 BGP configuration. Protected subnet `10.1.30.0/24` should have a Next Hop defined as Route**

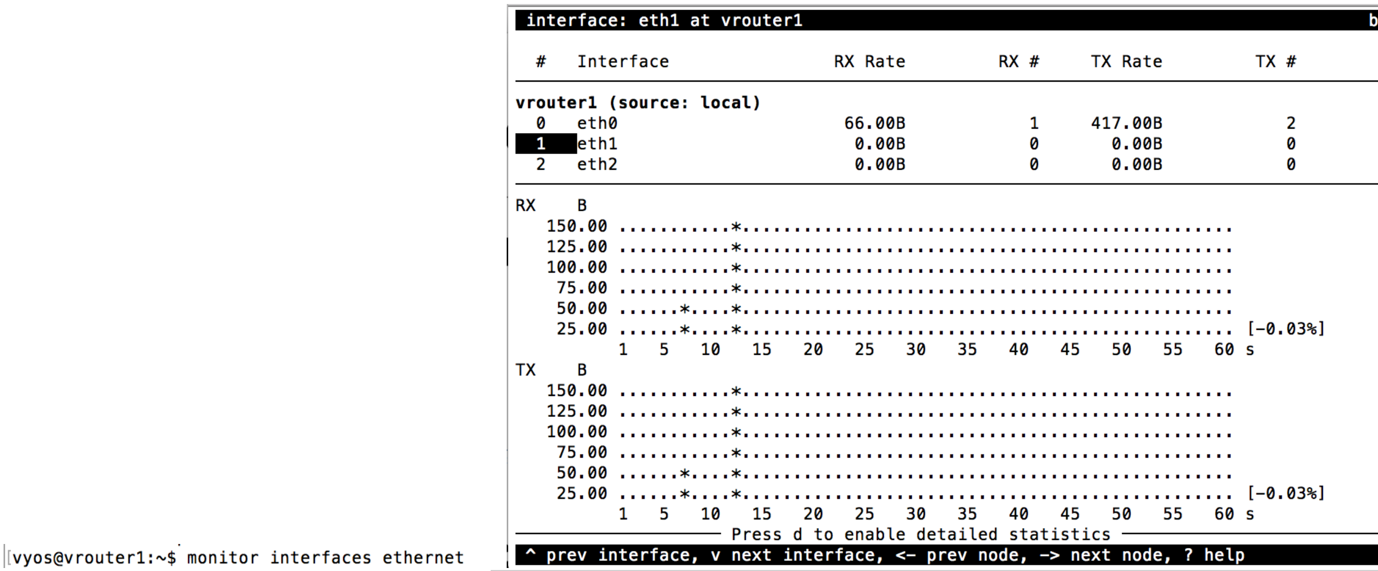
  ```
  show ip bgp
  ```

  ```
  vyos@vrouter1:~$ show ip bgp
  BGP table version is 0, local router ID is 10.1.10.243
  Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                r RIB-failure, S Stale, R Removed
  Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric LocPrf Weight Path
  *> 10.1.10.0/24     0.0.0.0                  1         32768 i
  *  10.1.30.0/24     10.1.20.244                            0 3 2 i
  *>                  10.1.20.244              1             0 2 i

  Total number of prefixes 2
  ```

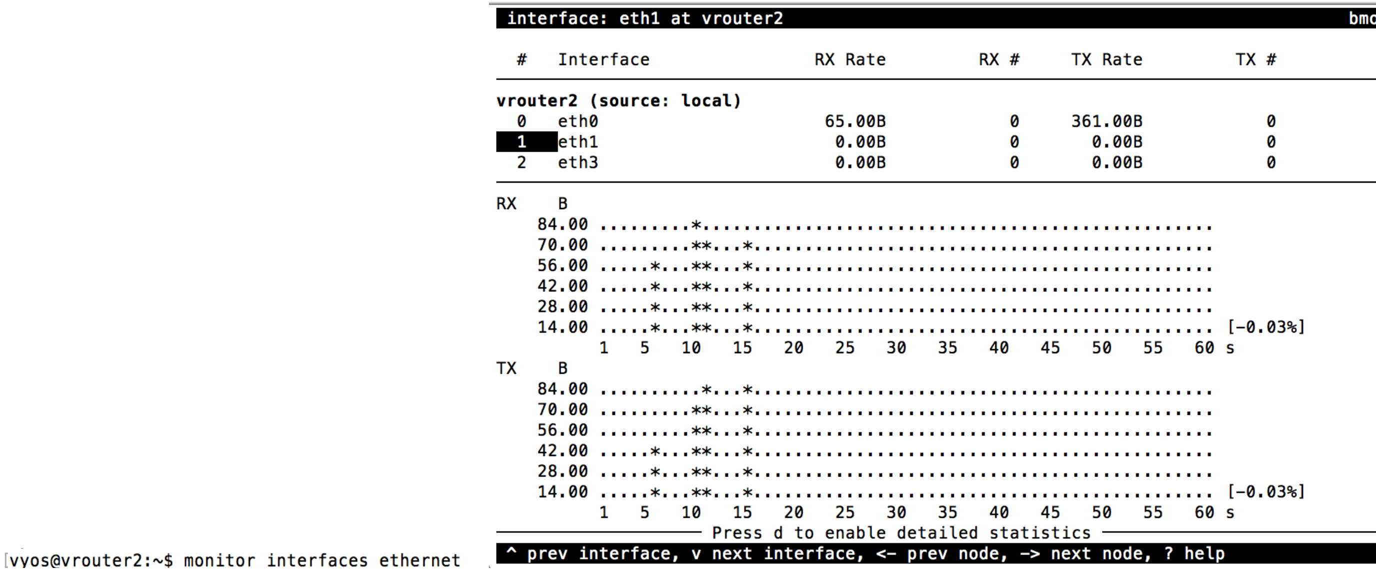
- Start interface monitoring in Router1 and Router2

```
monitor interfaces ethernet
```



```
vyos@vrouter1:~$ monitor interfaces ethernet
```

```
interface: eth1 at vrouter1                                                       b

  #   Interface                RX Rate         RX #    TX Rate         TX #

vrouter1 (source: local)
  0   eth0                      66.00B            1    417.00B            2
  1   eth1                       0.00B            0      0.00B            0
  2   eth2                       0.00B            0      0.00B            0

RX     B
   150.00 ...........*................................................
   125.00 ...........*................................................
   100.00 ...........*................................................
    75.00 ...........*................................................
    50.00 ......*....*................................................
    25.00 ......*....*................................................ [-0.03%]
          1   5   10   15   20   25   30   35   40   45   50   55   60 s
TX     B
   150.00 ...........*................................................
   125.00 ...........*................................................
   100.00 ...........*................................................
    75.00 ...........*................................................
    50.00 ......*....*................................................
    25.00 ......*....*................................................ [-0.03%]
          1   5   10   15   20   25   30   35   40   45   50   55   60 s
──────────────────── Press d to enable detailed statistics ────────────────────
 ^ prev interface, v next interface, <- prev node, -> next node, ? help
```



```
vyos@vrouter2:~$ monitor interfaces ethernet
```

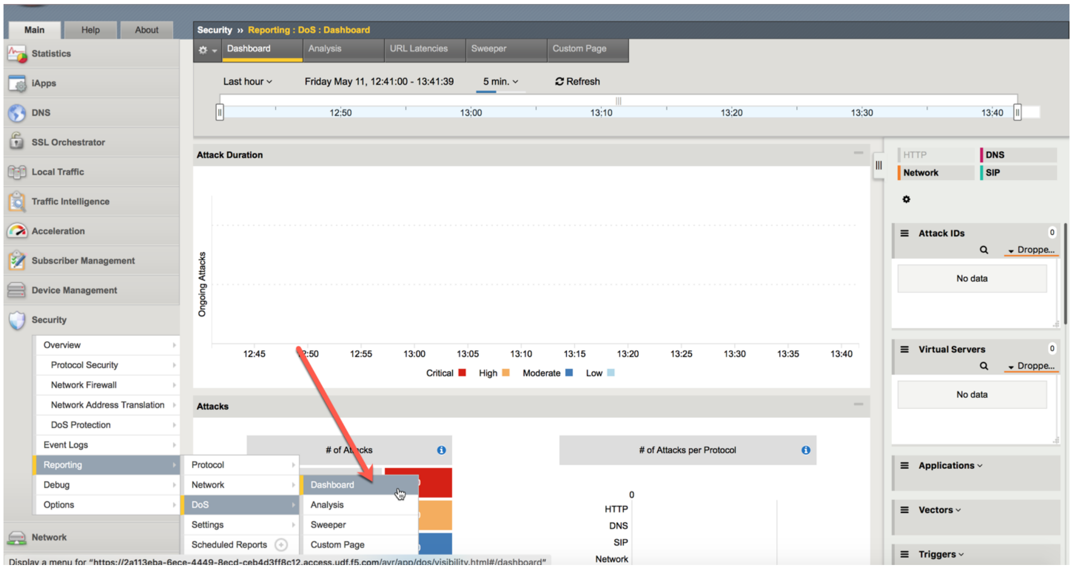
```
interface: eth1 at vrouter2                                                       bmc

  #   Interface                RX Rate         RX #    TX Rate         TX #

vrouter2 (source: local)
  0   eth0                      65.00B            0    361.00B            0
  1   eth1                       0.00B            0      0.00B            0
  2   eth3                       0.00B            0      0.00B            0

RX     B
    84.00 .........*..................................................
    70.00 .........**...*.............................................
    56.00 .....*...**...*.............................................
    42.00 .....*...**...*.............................................
    28.00 .....*...**...*.............................................
    14.00 .....*...**...*............................................. [-0.03%]
          1   5   10   15   20   25   30   35   40   45   50   55   60 s
TX     B
    84.00 ..........*...*.............................................
    70.00 .........**...*.............................................
    56.00 .........**...*.............................................
    42.00 .....*...**...*.............................................
    28.00 .....*...**...*.............................................
    14.00 .....*...**...*............................................. [-0.03%]
          1   5   10   15   20   25   30   35   40   45   50   55   60 s
──────────────────── Press d to enable detailed statistics ────────────────────
 ^ prev interface, v next interface, <- prev node, -> next node, ? help
```

- Select *eth1* and press `g` to enable graphical statistics

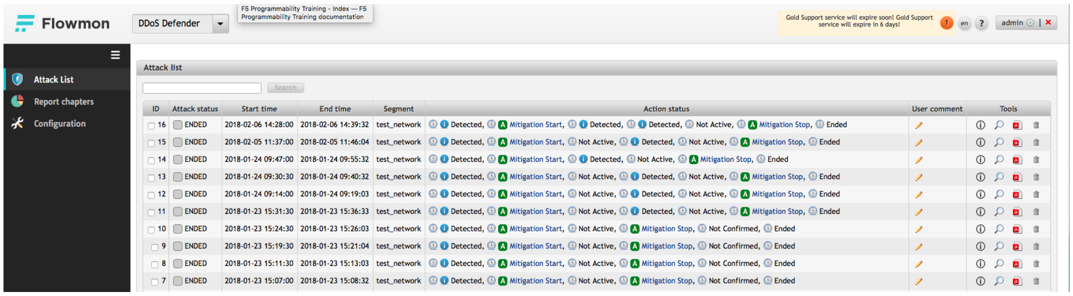
Note: You may need to expand terminal window for graphs to appear

---

- Open Web Browser and click on *BIG-IP AFM* bookmark, then login into BIG-IP TMUI using `admin` credentials
- Open **DoS Visibility Dashboard** in AFM TMUI



- In a new Browser tab click on *Flowmon Web interface* bookmark. Once Flowmon main menu opens, click on *Flowmon DDoS Defender* icon and login using `admin` credentials
- Open **Attack List** in Flowmon DDoS Defender WebUI


Flowmon
DDoS Defender
F5 Programmability Training - Index — F5 Programmability Training documentation
Gold Support service will expire soon! Gold Support service will expire in 6 days!
1
en
?
admin
Attack List
Report chapters
Configuration
Attack list
Search

ID	Attack status	Start time	End time	Segment	Action status	User comment	Tools
□ 16	ENDED	2018-02-06 14:28:00	2018-02-06 14:39:32	test_network	Detected, Mitigation Start, Detected, Detected, Not Active, Mitigation Stop, Ended		
□ 15	ENDED	2018-02-05 11:37:00	2018-02-05 11:46:04	test_network	Detected, Mitigation Start, Not Active, Detected, Not Active, Mitigation Stop, Ended		
□ 14	ENDED	2018-01-24 09:47:00	2018-01-24 09:55:32	test_network	Detected, Mitigation Start, Detected, Not Active, Mitigation Stop, Ended		
□ 13	ENDED	2018-01-24 09:30:30	2018-01-24 09:40:32	test_network	Detected, Mitigation Start, Not Active, Detected, Not Active, Mitigation Stop, Ended		
□ 12	ENDED	2018-01-24 09:14:00	2018-01-24 09:19:03	test_network	Detected, Mitigation Start, Not Active, Detected, Not Active, Mitigation Stop, Ended		
□ 11	ENDED	2018-01-23 15:31:30	2018-01-23 15:36:33	test_network	Detected, Mitigation Start, Not Active, Detected, Not Active, Mitigation Stop, Ended		
□ 10	ENDED	2018-01-23 15:24:30	2018-01-23 15:26:03	test_network	Detected, Mitigation Start, Not Active, Mitigation Stop, Not Confirmed, Ended		
□ 9	ENDED	2018-01-23 15:19:30	2018-01-23 15:21:04	test_network	Detected, Mitigation Start, Not Active, Mitigation Stop, Not Confirmed, Ended		
□ 8	ENDED	2018-01-23 15:11:30	2018-01-23 15:13:03	test_network	Detected, Mitigation Start, Not Active, Mitigation Stop, Not Confirmed, Ended		
□ 7	ENDED	2018-01-23 15:07:00	2018-01-23 15:08:32	test_network	Detected, Mitigation Start, Not Active, Mitigation Stop, Not Confirmed, Ended		

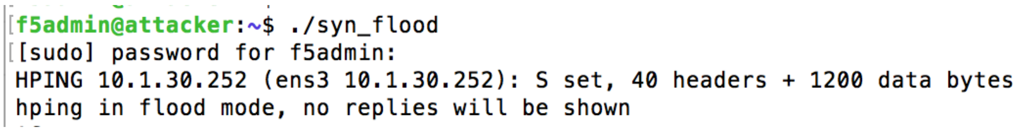
Note: Disregard any active alarms Flowmon may show in the upper right screen corner. These are artifcts of this lab environment

3.2 Initiate DDoS attack

3.2.1 Run SYN flood (hping3) from Attacker VM

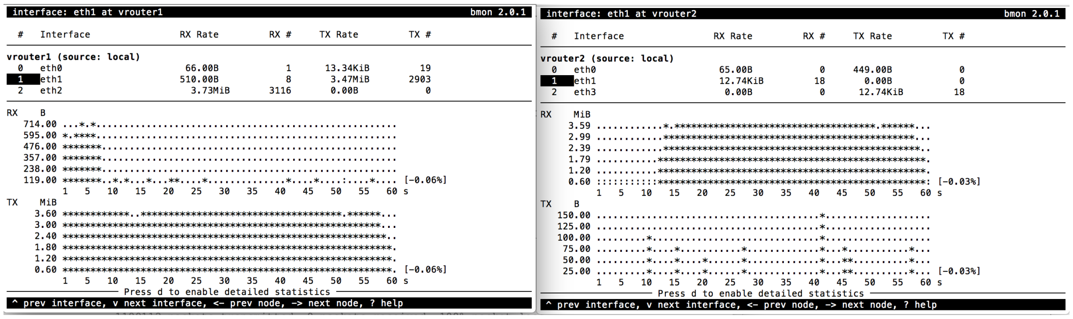
- Click on **Attacker SSH** icon to open `Attacker VM` ssh session
- From Attacker VM run SYN flood towards Web server

```
./syn_flood
```



```
f5admin@attacker:~$ ./syn_flood
[sudo] password for f5admin:
HPING 10.1.30.252 (ens3 10.1.30.252): S set, 40 headers + 1200 data bytes
hping in flood mode, no replies will be shown
```

- Observe traffic growth in both Router1 and Router2. After **15-45 seconds** traffic will drop in Router2 due to DDoS detection and mitigation start

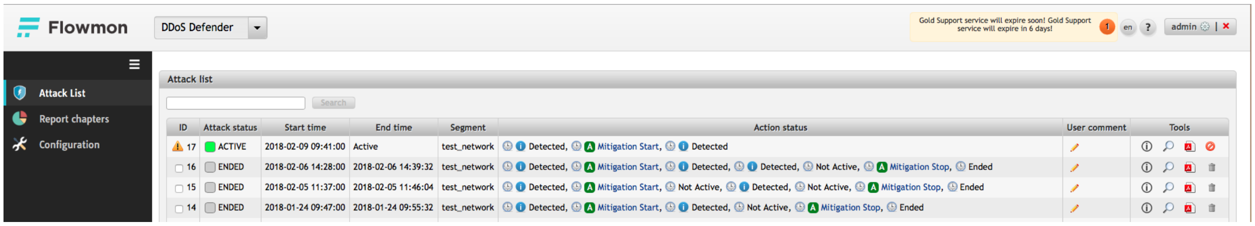


```
 interface: eth1 at vrouter1                                           bmon 2.0.1

  #   Interface                RX Rate         RX #     TX Rate         TX #

vrouter1 (source: local)
  0   eth0                      66.00B            1      13.34KiB         19
  1   eth1                     510.00B            8       3.47MiB       2903
  2   eth2                       3.73MiB       3116       0.00B            0

RX     B
   714.00 ...*.*......................................................
   595.00 *.****......................................................
   476.00 *******.....................................................
   357.00 *******.....................................................
   238.00 *******.....................................................
   119.00 *******..*.*...*...**....*.............*....*....:....*..... [-0.06%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
TX     MiB
     3.60 ************..************************************.******...
     3.00 *********************************************************...
     2.40 **********************************************************..
     1.80 ***********************************************************.
     1.20 ***********************************************************.
     0.60 ***********************************************************. [-0.06%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
────────────────────── Press d to enable detailed statistics ──────────────────────
 ^ prev interface, v next interface, <- prev node, -> next node, ? help
```

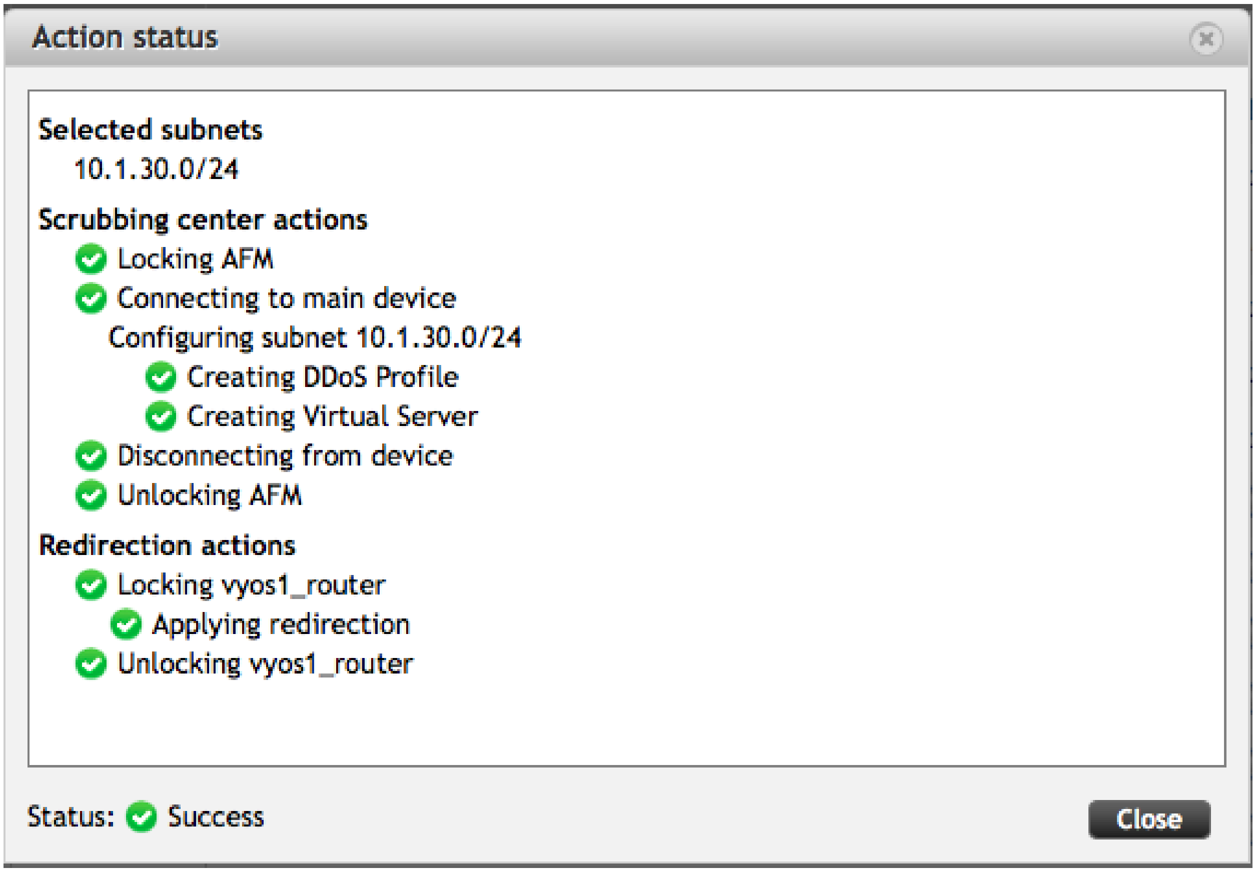
```
 interface: eth1 at vrouter2                                           bmon 2.0.1

  #   Interface                RX Rate         RX #     TX Rate         TX #

vrouter2 (source: local)
  0   eth0                      65.00B            0     449.00B            0
  1   eth1                      12.74KiB         18       0.00B            0
  2   eth3                       0.00B            0      12.74KiB         18

RX     MiB
     3.59 ............*.************************************.******...
     2.99 ............*********************************************...
     2.39 ............**********************************************..
     1.79 ...........************************************************.
     1.20 ...........************************************************.
     0.60 :::::::::::************************************************: [-0.03%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
TX     B
   150.00 ........................................*...................
   125.00 ........................................*...................
   100.00 .........*..............................*...................
    75.00 .........*....*...........*.............*...*...........*...
    50.00 .........*....*....*......*.............*...**..........*...
    25.00 .........*....*....*......*.............*...**..........*... [-0.03%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
────────────────────── Press d to enable detailed statistics ──────────────────────
 ^ prev interface, v next interface, <- prev node, -> next node, ? help
```

3.2.2 DDoS mitigation start

An *ACTIVE* attack with the new ID will appear in Flowmon DDoS defender 'Active attacks' screen. Flowmon dynamically provisions AFM DDoS profile and VS, and initiates traffic diversion to AFM using BGP advertisement



ID	Attack status	Start time	End time	Segment	Action status	User comment	Tools
17	🟩 ACTIVE	2018-02-09 09:41:00	Active	test_network	Detected, Mitigation Start, Detected		
□ 16	ENDED	2018-02-06 14:28:00	2018-02-06 14:39:32	test_network	Detected, Mitigation Start, Detected, Detected, Not Active, Mitigation Stop, Ended		
□ 15	ENDED	2018-02-05 11:37:00	2018-02-05 11:46:04	test_network	Detected, Mitigation Start, Not Active, Detected, Not Active, Mitigation Stop, Ended		
□ 14	ENDED	2018-01-24 09:47:00	2018-01-24 09:55:32	test_network	Detected, Mitigation Start, Detected, Not Active, Mitigation Stop, Ended		



Action status

Selected subnets

10.1.30.0/24

Scrubbing center actions

- ✓ Locking AFM
- ✓ Connecting to main device
  - Configuring subnet 10.1.30.0/24
    - ✓ Creating DDoS Profile
    - ✓ Creating Virtual Server
- ✓ Disconnecting from device
- ✓ Unlocking AFM

Redirection actions

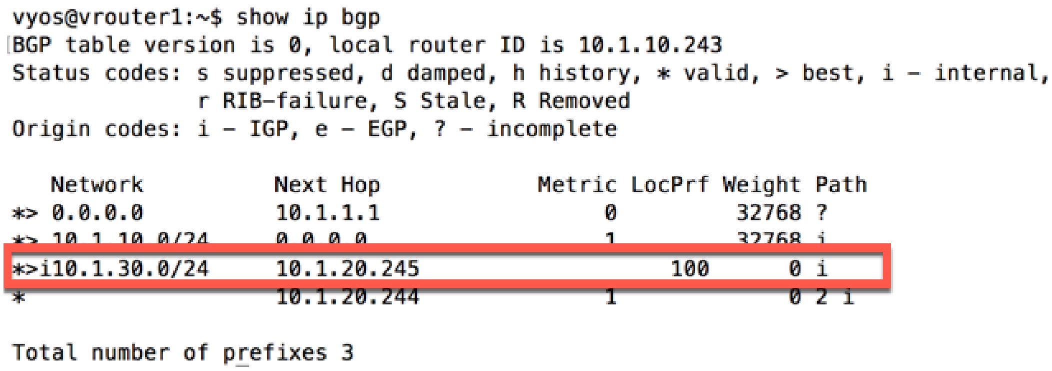
- ✓ Locking vyos1_router
  - ✓ Applying redirection
- ✓ Unlocking vyos1_router

Status: ✓ Success

3.2.3 BGP route change and traffic drop

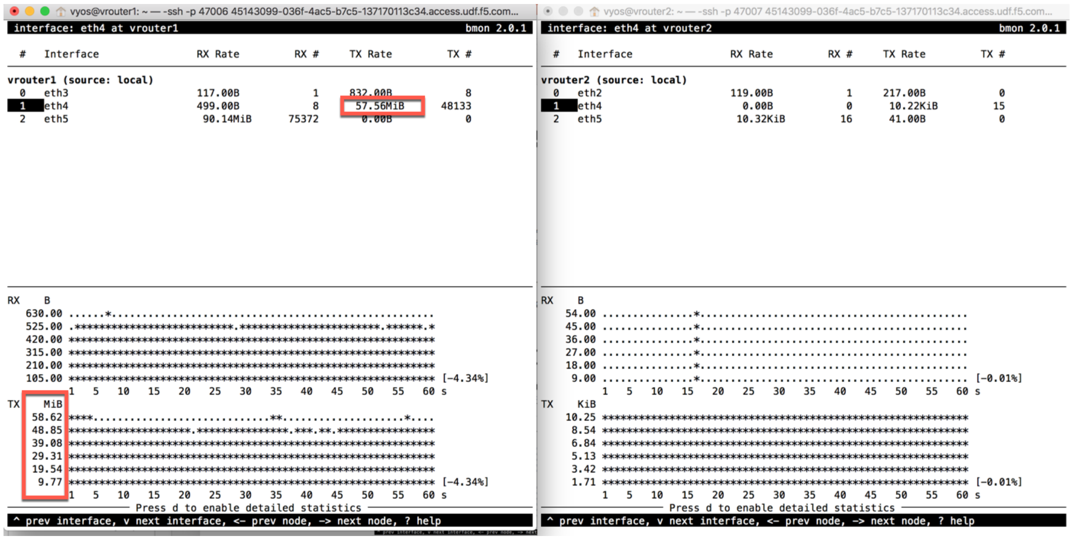
- Router1 shows new route to protected `10.1.30.0/24` subnet

  ```
  show ip bgp
  ```



```
vyos@vrouter1:~$ show ip bgp
BGP table version is 0, local router ID is 10.1.10.243
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          10.1.1.1                 0         32768 ?
*> 10.1.10.0/24     0.0.0.0                  1         32768 i
*>i10.1.30.0/24     10.1.20.245                   100      0 i
*                   10.1.20.244              1             0 2 i

Total number of prefixes 3
```

- As traffic is being routed through AFM, Router2 shows no significant network activity while Router1 still experiences high traffic load



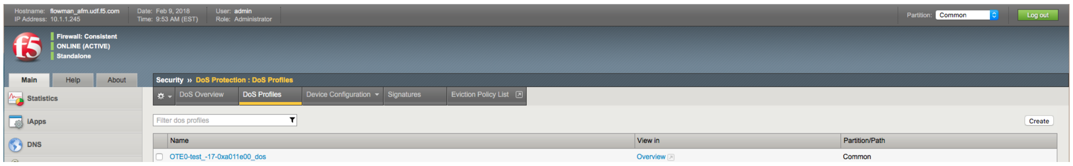
```
vyos@vrouter1: ~ — -ssh -p 47006 45143099-036f-4ac5-b7c5-137170113c34.access.udf.f5.com...
interface: eth4 at vrouter1                                          bmon 2.0.1

 #   Interface                RX Rate         RX #     TX Rate         TX #

vrouter1 (source: local)
 0   eth3                     117.00B            1     832.00B            8
 1   eth4                     499.00B            8      57.56MiB      48133
 2   eth5                      90.14MiB      75372       0.00B            0

RX     B
   630.00 ......*.....................................................
   525.00 .**************************.***********************.******.*
   420.00 ************************************************************
   315.00 ************************************************************
   210.00 ************************************************************
   105.00 ************************************************************ [-4.34%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
TX      MiB
    58.62 ****.............................**....................*....
    48.85 ********************.***************.***.**.****************
    39.08 ************************************************************
    29.31 ************************************************************
    19.54 ************************************************************
     9.77 ************************************************************ [-4.34%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
──────────────── Press d to enable detailed statistics ────────────────
^ prev interface, v next interface, <- prev node, -> next node, ? help
```

```
vyos@vrouter2: ~ — -ssh -p 47007 45143099-036f-4ac5-b7c5-137170113c34.access.udf.f5.com...
interface: eth4 at vrouter2                                          bmon 2.0.1

 #   Interface                RX Rate         RX #     TX Rate         TX #

vrouter2 (source: local)
 0   eth2                     119.00B            1     217.00B            0
 1   eth4                       0.00B            0      10.22KiB         15
 2   eth5                      10.32KiB         16      41.00B            0

RX     B
    54.00 ...............*............................................
    45.00 ...............*............................................
    36.00 ...............*............................................
    27.00 ...............*............................................
    18.00 ...............*............................................
     9.00 ...............*............................................ [-0.01%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
TX     KiB
    10.25 ************************************************************
     8.54 ************************************************************
     6.84 ************************************************************
     5.13 ************************************************************
     3.42 ************************************************************
     1.71 ************************************************************ [-0.01%]
          1   5    10   15   20   25   30   35   40   45   50   55   60 s
──────────────── Press d to enable detailed statistics ────────────────
^ prev interface, v next interface, <- prev node, -> next node, ? help
```

3.2.4 AFM DDoS profile and virtual server

Note: Flowmon uses iControl REST interface to provision necessary parameters in AFM

- In AFM TMUI Navigate to **Security –> DoS protection –> DoS profiles** and confirm that the DoS profile has been provisioned for the protected subnet



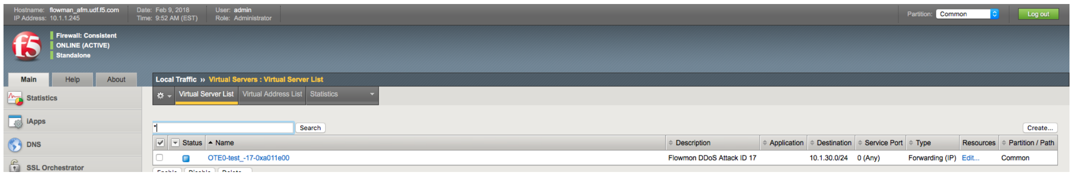
Hostname: flowman_afm.udf.f5.com
IP Address: 10.1.1.245
Date: Feb 9, 2018
Time: 9:53 AM (EST)
User: admin
Role: Administrator
Partition: Common

Firewall: Consistent
ONLINE (ACTIVE)
Standalone

Security » DoS Protection : DoS Profiles

	Name	View in	Partition/Path
□	OTE0-test_-17-0xa011e00_dos	Overview	Common

- In **Local Traffic –> Virtual Servers –> Virtual Server List** confirm that VS with corresponding Attack ID has been created



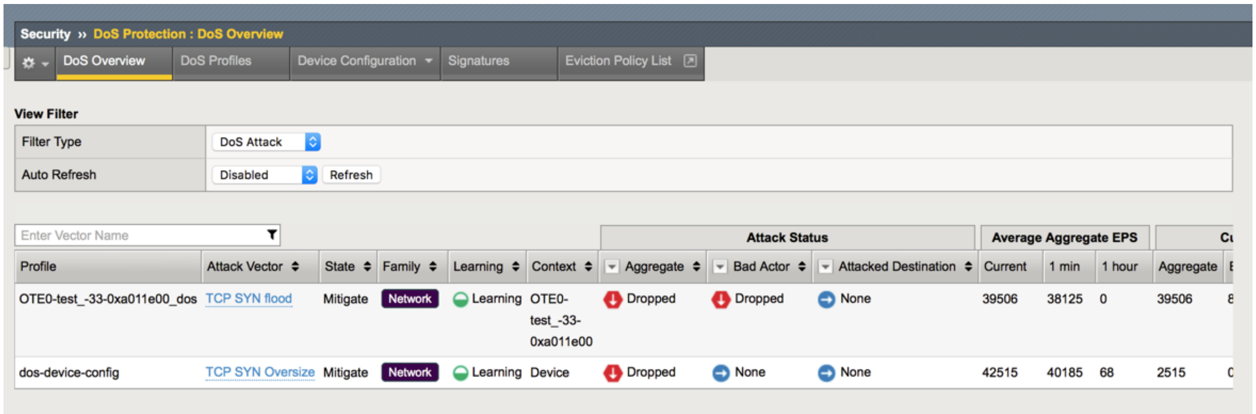
Hostname: flowman_afm.udf.f5.com
IP Address: 10.1.1.245
Date: Feb 9, 2018
Time: 9:52 AM (EST)
User: admin
Role: Administrator
Partition: Common

Local Traffic » Virtual Servers : Virtual Server List

Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
	OTE0-test_-17-0xa011e00	Flowmon DDoS Attack ID 17		10.1.30.0/24	0 (Any)	Forwarding (IP)	Edit...	Common

3.2.5 AFM DDoS mitigation

In AFM TMUI navigate to **Security –> DoS Protection –> DoS Overview** and confirm that AFM is performing DoS mitigation using the provisioned DoS profile



Security » DoS Protection : DoS Overview

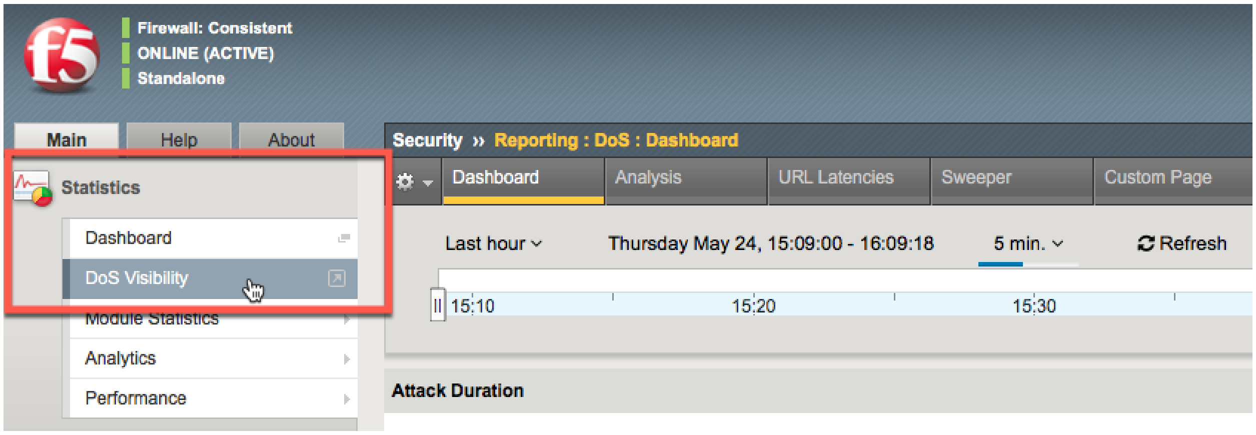
View Filter

Filter Type	DoS Attack
Auto Refresh	Disabled

						Attack Status			Average Aggregate EPS			Cu	
Profile	Attack Vector	State	Family	Learning	Context	Aggregate	Bad Actor	Attacked Destination	Current	1 min	1 hour	Aggregate	E
OTE0-test_-33-0xa011e00_dos	TCP SYN flood	Mitigate	Network	Learning	OTE0-test_-33-0xa011e00	Dropped	Dropped	None	39506	38125	0	39506	8
dos-device-config	TCP SYN Oversize	Mitigate	Network	Learning	Device	Dropped	None	None	42515	40185	68	2515	0

Note: *Statistics -> DoS Visibility* TMUI menu provides graphical attack data

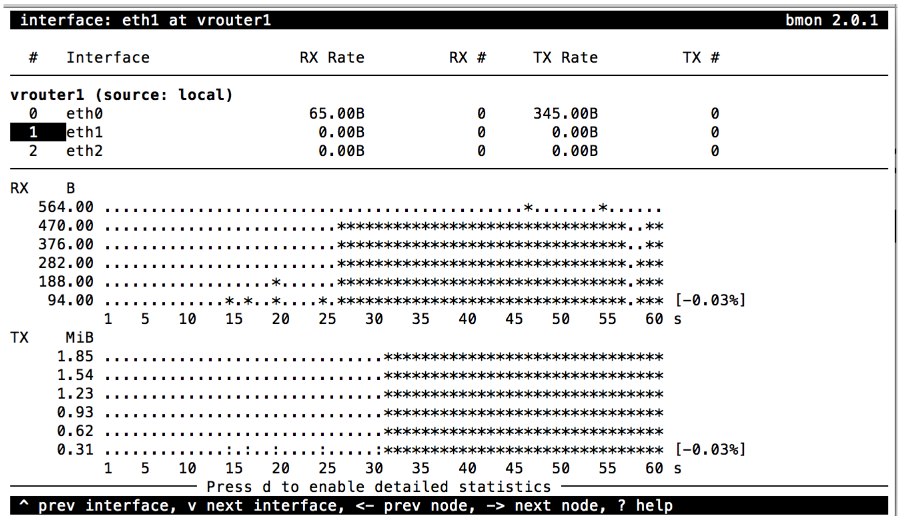
It may take up to ~5 minutes for DoS Visibility Dashboard to show our simulated DDoS attack. You may need to click *Refresh* for data to appear



3.3 Attack stop

3.3.1 Stop SYN flood

Press (`Ctrl-C`) to finish the attack. Traffic will drop on Router1

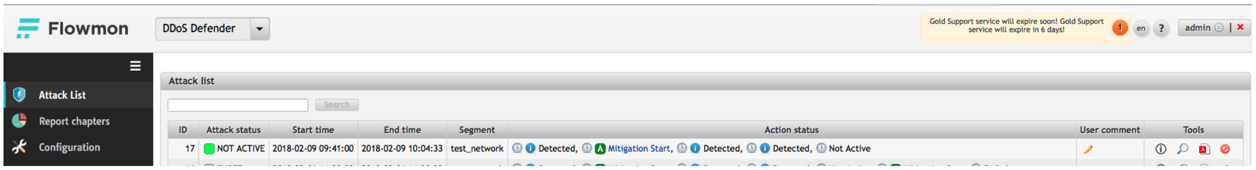


```
 interface: eth1 at vrouter1                                                       bmon 2.0.1

  #   Interface                RX Rate         RX #     TX Rate         TX #

vrouter1 (source: local)
  0   eth0                      65.00B            0     345.00B            0
  1   eth1                       0.00B            0       0.00B            0
  2   eth2                       0.00B            0       0.00B            0

RX     B
   564.00 .............................................*.......*......
   470.00 .........................*******************************..**
   376.00 .........................*******************************..**
   282.00 .........................*******************************.***
   188.00 ..................*......*******************************.***
    94.00 .............*.*..*....*.*******************************.*** [-0.03%]
          1   5   10   15   20   25   30   35   40   45   50   55   60 s
TX     MiB
     1.85 ..............................******************************
     1.54 ..............................******************************
     1.23 ..............................******************************
     0.93 ..............................******************************
     0.62 ..............................******************************
     0.31 .............:.:..:....:.....:****************************** [-0.03%]
          1   5   10   15   20   25   30   35   40   45   50   55   60 s
───────────────────────── Press d to enable detailed statistics ───────────────────────────
 ^ prev interface, v next interface, <- prev node, -> next node, ? help
```

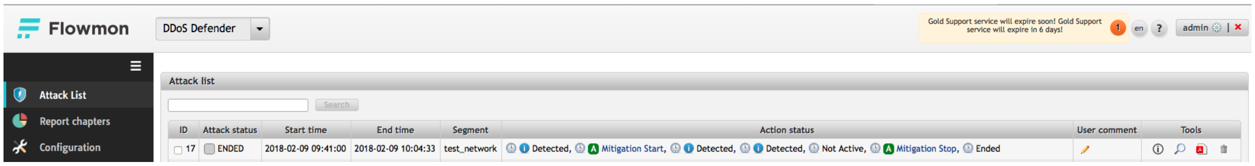
Note: STOP HERE. It will take 5-10 minutes for Flowmon to mark the attack as *NOT ACTIVE*. This is done in order to avoid 'flip-flop' effect in repeated attack situation

3.3.2 Mitigation stop

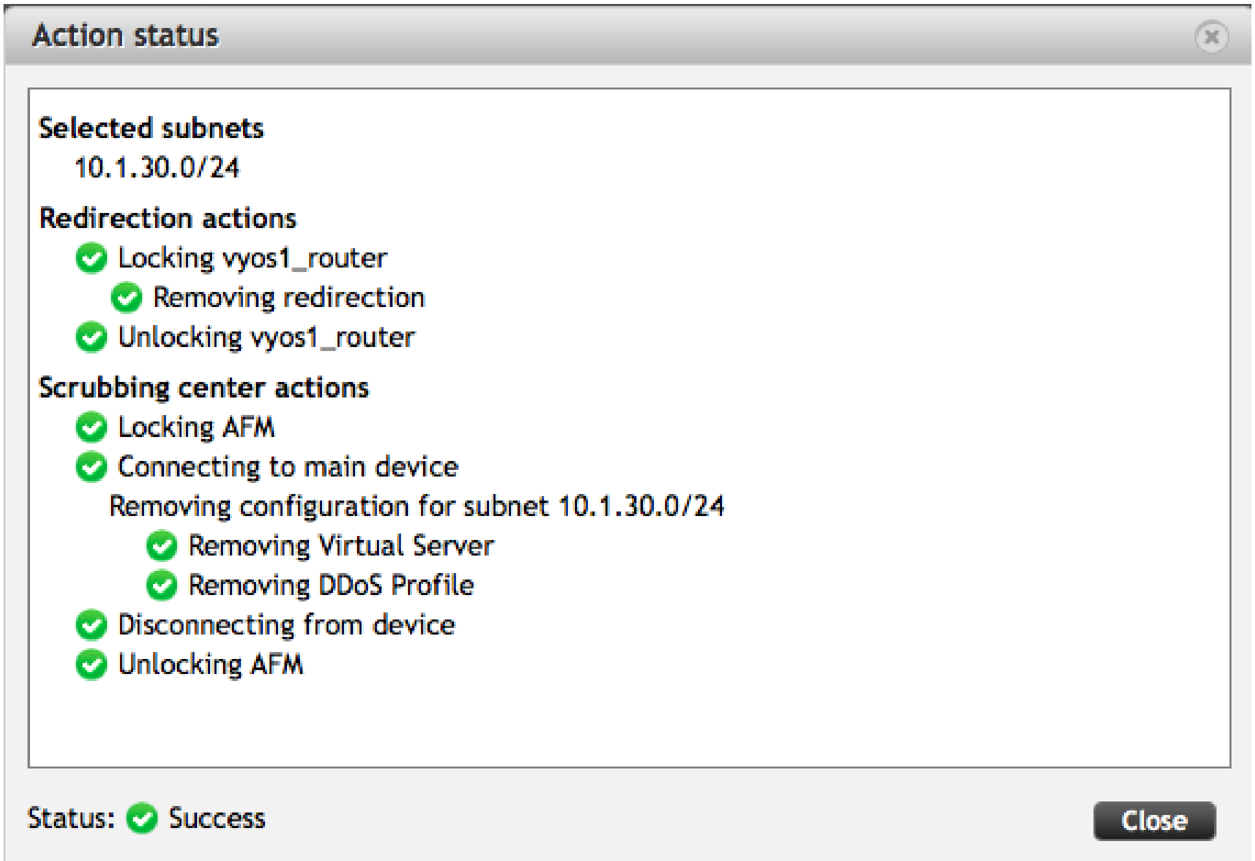
Flowmon DDoS Defender Attack List screen shows the current attack with status *NOT ACTIVE*. Attack will transition to *ENDED* state when Flowmon performs *Mitigation Stop* routine



ID	Attack status	Start time	End time	Segment	Action status	User comment	Tools
17	🟩 NOT ACTIVE	2018-02-09 09:41:00	2018-02-09 10:04:33	test_network	Detected, A Mitigation Start, Detected, Detected, Not Active		



ID	Attack status	Start time	End time	Segment	Action status	User comment	Tools
□ 17	□ ENDED	2018-02-09 09:41:00	2018-02-09 10:04:33	test_network	Detected, A Mitigation Start, Detected, Detected, Not Active, A Mitigation Stop, Ended		



Action status

Selected subnets
- 10.1.30.0/24

Redirection actions
- ✓ Locking vyos1_router
  - ✓ Removing redirection
- ✓ Unlocking vyos1_router

Scrubbing center actions
- ✓ Locking AFM
- ✓ Connecting to main device
  - Removing configuration for subnet 10.1.30.0/24
    - ✓ Removing Virtual Server
    - ✓ Removing DDoS Profile
- ✓ Disconnecting from device
- ✓ Unlocking AFM

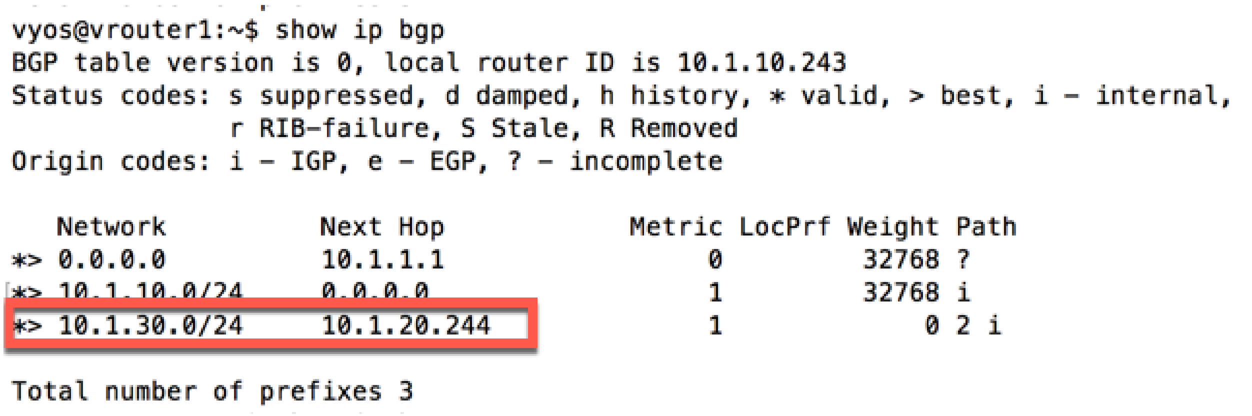
Status: ✓ Success

**It typically takes ~ 5min for Flowmon DDoS Defender to update attack status*

3.3.3 AFM configuration, BGP route removal

As part of *Mitigation Stop* routine Flowmon removes BGP route from Router1 and Virtual Server and DDoS Profile from AFM

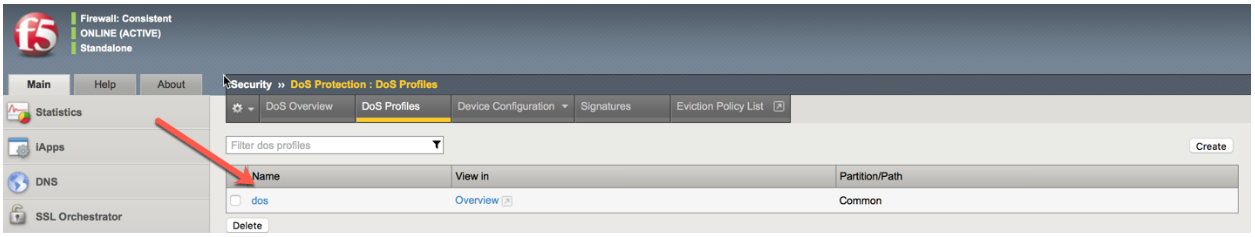
```
show ip bgp
```



```
vyos@vrouter1:~$ show ip bgp
BGP table version is 0, local router ID is 10.1.10.243
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          10.1.1.1                 0         32768 ?
*> 10.1.10.0/24     0.0.0.0                  1         32768 i
*> 10.1.30.0/24     10.1.20.244              1             0 2 i

Total number of prefixes 3
```

In AFM TMUI navigate to Security –> DoS Protection –> DoS Profiles

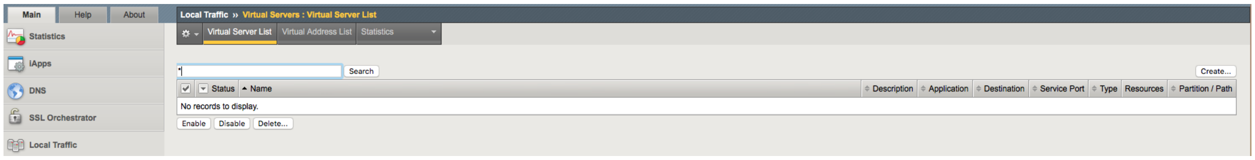
Verify that only default “dos” profile present



Name	View in	Partition/Path
dos	Overview	Common

In AFM TMUI navigate to Local Traffic –> Virtual Servers –> Virtual Server List

Verify that Virtual Server matching Attack ID has been removed



Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
No records to display.								

Congratulations! You have successfully completed the lab!